

# Confluence by Decreasing Diagrams – Formalized\*

Harald Zankl

Institute of Computer Science, University of Innsbruck, 6020 Innsbruck, Austria

---

## Abstract

Decreasing diagrams are a complete characterization of confluence for abstract rewrite systems whose convertibility classes are countable. In this paper we present a formalization of decreasing diagrams in the theorem prover Isabelle. The main contribution is a formal proof that any locally decreasing abstract rewrite system is confluent.

**1998 ACM Subject Classification** F.3.1, F.4.2

**Keywords and phrases** term rewriting, confluence, decreasing diagrams, formalization

## 1 Introduction

Formalizing confluence criteria has a long history in  $\lambda$ -calculus. Huet [9] proved a stronger variant of the parallel moves lemma in Coq. Isabelle/HOL was used in [14] to prove the Church-Rosser property of  $\beta$ ,  $\eta$ , and  $\beta\eta$ . For  $\beta$ -reduction the standard Tait/Martin-Löf proof as well as Takahashi’s proof [27] were formalized. The first mechanically verified proof of the Church-Rosser property of  $\beta$ -reduction was done using the Boyer-Moore theorem prover [24]. The formalization in Twelf [21] was used to formalize the confluence proof of a specific higher-order rewrite system in [26].

Newman’s lemma (for abstract rewrite systems) and Knuth and Bendix’ critical pair theorem (for first-order rewrite systems) have been proved in [23] using ACL. An alternative proof of the latter in PVS, following the higher-order structure of Huet’s proof, is presented in [7]. PVS is also used in the formalization of the lemmas of Newman and Yokouchi in [6]. Knuth and Bendix’ criterion has also been formalized in Coq [3] and Isabelle [29].

Decreasing diagrams [17] are a complete characterization of confluence for abstract rewrite systems whose convertibility classes are countable. As a criterion for abstract rewrite systems, they can easily be applied for first- and higher-order rewriting, including term rewriting and the  $\lambda$ -calculus. Furthermore, decreasing diagrams yield constructive proofs of confluence [20] (in the sense that the joining sequences can be computed based on the divergence). We are not aware of a (complete) formalization of decreasing diagrams in any theorem prover (see remarks in Section 5).

In this paper we discuss a formalization of decreasing diagrams in the theorem prover Isabelle/HOL. (In the sequel we just call it Isabelle.) We closely follow the original proof [17]. For alternative proofs see [1, 11, 19] or [10, 16, 5] where proof orders play an essential role. The main contribution of this paper is a mechanical proof of the following theorem in Isabelle.

► **Theorem 1** (van Oostrom [17]). *A locally decreasing abstract rewrite system is confluent.*

To achieve this goal we had to identify (and fix some) omissions in [17] and had to give formal proofs of all intermediate results. As a consequence all lemmata in this paper have been formally proven in Isabelle. Our formalization consists of approximately 1000 lines of Isabelle code in the Isar style and contains 22 definitions and 97 lemmata. It is available

---

\* This research is supported by FWF P22467.

meaning	set	multiset	sequence/list	[17]
empty	$\{\}$	$\{\#\}$	$[\ ]$	$\emptyset/\epsilon$
singleton	$\{x\}$	$\{\#x\# \}$	$[x]$	$\{x\}/[x]/x$
membership	$x \in S$	$x \in \# M$	–	$\in$
union/concatenation	$S \cup T$	$M + N$	$\sigma @ \tau$	$\uplus / \sigma \tau$
intersection	$S \cap T$	$M \# \cap N$	–	$\cap$
difference	$S - T$	$M - N$	–	–
sub(multi)set	$S \subseteq T$	$M \leq N$	–	$\subseteq$

■ **Table 1** Predefined Isabelle operators.

from [http://cl-informatik.uibk.ac.at/users/hzankl/Decreasing\\_Diagrams.thy](http://cl-informatik.uibk.ac.at/users/hzankl/Decreasing_Diagrams.thy). It requires Isabelle 2012 and the Archive of Formal Proofs<sup>1</sup> from July 30, 2012.

The remainder of this paper is organized as follows. In the next section we recall some preliminaries that are helpful to understand our formalization, which is described in Section 3. In Section 4 we highlight changes to (and omissions in) the proofs from [17] before we conclude in Section 5.

## 2 Preliminaries

We assume familiarity with rewriting [28] and the original proof of decreasing diagrams [17]. Basic knowledge of Isabelle [15] is not essential but may be helpful. Our formalization imports the theory `Multiset.thy` from the Isabelle library and `Abstract_Rewriting.thy` from the Archive of Formal Proofs (see [25]).

In Isabelle an *abstract rewrite system* (ARS) is a set of pairs of objects of the same type, i.e., a binary relation. We introduce *labeled* ARSs in Section 3.4.

We will use  $\mathcal{A}$  ( $\mathcal{B}$ ) for (labeled) ARSs and denote sets by  $S, T, U$ , multisets by  $M, N, I, J, K, Q$ , single labels by  $\alpha$  and  $\beta$ , and lists of labels by  $\sigma, \tau, \upsilon, \rho$ , and  $\kappa$  (possibly primed).

Table 1 gives an overview of several predefined operators in Isabelle for sets, multisets, and lists where we also incorporated the notation from [17] in the rightmost column. In addition we need the difference (intersection) of a multiset with a set. Here  $M -_s S$  ( $M \cap_s S$ ) removes (keeps) all occurrences of elements in  $M$  that are in  $S$ . In the paper we will use the Isabelle notation, but drop the  $@$  for concatenating sequences.

Then we can easily establish the following relationships:

► **Lemma 2** (parts of [17, Lemma A.3]).

1.  $(M + N) -_s S = (M -_s S) + (N -_s S)$
2.  $(M -_s S) -_s T = M -_s (S \cup T)$
3.  $M = (M \cap_s S) + (M -_s S)$
4.  $(M -_s T) \cap_s S = (M \cap_s S) -_s T$

**Proof.** By definition of multiset and the operators. ◀

Sometimes it will be necessary to convert e.g. a multiset to a set. In Isabelle we will use the functions `set/set_of`, and `multiset_of`, which convert a list/multiset into a set, and a list into a multiset, respectively. In the paper we leave these conversions implicit, since no confusion can arise.

<sup>1</sup> <http://afp.sourceforge.net/download.shtml>

### 3 Formalization of Decreasing Diagrams

We assume familiarity with the original proof of decreasing diagrams in [17], upon which our formalization is based. Nevertheless we will recall the important definitions and lemmata. However, we only give proofs if our proof deviates from the original argument. In addition we state (sometimes small) key results, since an effective collection of lemmata is crucial for completely formal proofs.

The remainder of this section is organized as follows: Section 3.1 describes our results on multisets. Section 3.2 is dedicated to decreasingness (of labels) and Section 3.3 is concerned with an alternative formulation of local decreasingness. Afterwards, Section 3.4 lifts decreasingness (from labels) to diagrams. Well-foundedness of the measure on peaks is proved in Section 3.5, which is needed for the main result in Section 3.6. As an application of decreasing diagrams we have formally proved Newman’s Lemma [13] in Section 3.7.

#### 3.1 Multisets

In the sequel we assume  $\prec$  to be transitive and irreflexive.

► **Definition 3** ([17, Definition 2.5]).

1. The set  $\Upsilon\alpha$  is the strict order ideal generated by (or *down-set* of)  $\alpha$ , defined by  $\Upsilon\alpha = \{\beta \mid \beta \prec \alpha\}$ . This is extended to sets  $\Upsilon S = \bigcup_{x \in S} \Upsilon x$ . We define  $\Upsilon M$  and  $\Upsilon\sigma$  to be the down-set generated by the set of elements in  $M$  and  $\sigma$ , respectively.
2. The (*standard*) *multiset extension* (denoted by  $\prec_{\text{mul}}$ ) of  $\prec$  is defined by

$$M \prec_{\text{mul}} N \text{ if } \exists I \ J \ K. \ M = I + K, \ N = I + J, \ K \subseteq \Upsilon J, \text{ and } J \neq \{\#\}$$

The relation  $\prec_{\text{mul}}$  is obtained by removing the last condition ( $J \neq \{\#\}$ ). Note that  $\preccurlyeq_{\text{mul}}$  is the reflexive closure of  $\prec_{\text{mul}}$ .<sup>2</sup>

This definition can easily be mimicked in Isabelle (here **ds/dm/dl** defines the down-set for a set/multiset/list):<sup>3</sup>

```

definition ds :: "'a rel  $\Rightarrow$  'a set  $\Rightarrow$  'a set"
  where "ds r S = {y .  $\exists$ x  $\in$  S. (y,x)  $\in$  r}"

definition dm :: "'a rel  $\Rightarrow$  'a multiset  $\Rightarrow$  'a set"
  where "dm r M = ds r (set_of M)"

definition dl :: "'a rel  $\Rightarrow$  'a list  $\Rightarrow$  'a set"
  where "dl r  $\sigma$  = ds r (set  $\sigma$ )"

definition mul :: "'a rel  $\Rightarrow$  'a multiset rel" where
  "mul r = {(M,N).  $\exists$ I J K. M = I + K  $\wedge$  N = I + J  $\wedge$  set_of K  $\subseteq$  dm r J  $\wedge$  J  $\neq$  {\#}}"

definition mul_eq :: "'a rel  $\Rightarrow$  'a multiset rel" where
  "mul_eq r = {(M,N).  $\exists$ I J K. M = I + K  $\wedge$  N = I + J  $\wedge$  set_of K  $\subseteq$  dm r J}"

```

We establish the following easy result on the down-set, which is not mentioned in [17] but turned out to be handy for our formalization:

<sup>2</sup> See Lemma 32 in Section 4.

<sup>3</sup> For readability of subsequent definitions we denote  $\prec$  by **r** within code listings.

► **Lemma 4.**  $\Upsilon(\Upsilon S) \subseteq \Upsilon S$

**Proof.** Assume  $x \in \Upsilon(\Upsilon S)$ . Then there must be a  $y \in \Upsilon S$  with  $x \prec y$ . From  $y \in \Upsilon S$  we get a  $z \in S$  with  $y \prec z$ . Then  $x \prec z$  by transitivity and hence  $x \in \Upsilon S$ . ◀

The multiset extension inherits some properties of the base relation, which we will implicitly use in the sequel.

► **Lemma 5.** *Let  $\prec$  be a transitive and well-founded relation. Then  $\prec_{mul}$  is transitive and well-founded, and  $\preceq_{mul}$  is reflexive and transitive.*

**Proof.** All these properties follow from Lemma 31 (Section 4) in combination with existing results in `Multiset.thy`. ◀

We can now establish the following properties.

► **Lemma 6** ([17, Lemma 2.6]).

1.  $\Upsilon(S \cup T) = \Upsilon S \cup \Upsilon T$  and  $\Upsilon(\sigma\tau) = \Upsilon\sigma \cup \Upsilon\tau$  and  $\Upsilon(M -s S) \supseteq \Upsilon M -s \Upsilon S$
2.  $M \leq N \Rightarrow M \preceq_{mul} N \Rightarrow \Upsilon M \subseteq \Upsilon N$
3.  $M \preceq_{mul} N \Rightarrow \exists I \ J \ K. N = I + J \wedge M = I + K \wedge J \# \cap K = \# \wedge K \subseteq \Upsilon J$
4.  $N \neq \{\#\} \wedge M \subseteq \Upsilon N \Rightarrow M \preceq_{mul} N$
5.  $M \preceq_{mul} N \Rightarrow M -s \Upsilon S \preceq_{mul} N -s \Upsilon S$
6.  $M \preceq_{mul} N \Leftrightarrow Q + M \preceq_{mul} Q + N$
7.  $Q \subseteq \Upsilon N - \Upsilon M \wedge M \preceq_{mul} N \Rightarrow Q + M \preceq_{mul} N$
8.  $S \subseteq T \Rightarrow M -s T \preceq_{mul} M -s S$
9.  $M \prec_{mul} N \Rightarrow Q + M \prec_{mul} Q + N$

**Proof.**

3. Assume  $M = I + K$ ,  $N = I + J$ , and  $K \subseteq \Upsilon J$ . Take  $I' = I + (J \# \cap K)$ ,  $K' = K - (J \# \cap K)$ , and  $J' = J - (J \# \cap K)$ . Obviously  $K'$  and  $J'$  are disjoint. The result follows from:

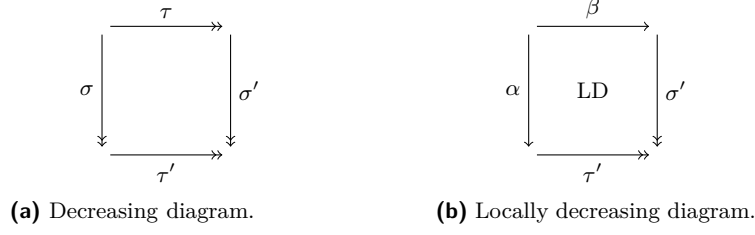
$$K \subseteq \Upsilon J \Rightarrow K' \subseteq \Upsilon J'$$

To show the result we fix a  $k \in \# K - (J \# \cap K)$ . Obviously  $k \in \# K$  and we show that for any  $K'$  we have  $K' \leq K \Rightarrow k \in \Upsilon(J - K')$  by induction (on  $K'$ ) on finite multisets. Hence  $k \in \Upsilon(J - K)$  and we conclude by the observation that  $J - K = J - (J \# \cap K)$ .

5. Follows from [17, Lemma 2.6(5)] using Lemma 4.
6. Immediate from [17, Lemma 2.6(6)].
8. From the hypothesis we get  $M -s T \leq M -s S$  which yields the result from item (2).
9. By definition of  $\prec_{mul}$ .

The other items are proved as in [17]. ◀

Note that statements (5) and (6) slightly differ from [17, Lemma 2.6](5,6), but are easier to apply. However, the statements of (8) and (9) are not mentioned in [17], which we required to replay [17, Lemmata 3.5 and 3.6].



■ **Figure 1** Diagrams.

### 3.2 Decreasingness

We define the *lexicographic maximum* measure, which maps lists to multisets, inductively.

► **Definition 7** ([17, Definition 3.2]).

- $|[]| = \{\#\}$
- $|\alpha\sigma| = \{\#\alpha\#\} + (|\sigma| - s \gamma \alpha)$

Since the lexicographic maximum measure depends on the base order  $\prec$  on labels, in Isabelle this definition amounts to:

```
fun lexmax :: "'a rel ⇒ 'a list ⇒ 'a multiset" ("(_|_)" ) where
  "r|[]| = {#}"
  | "r|α#σ| = {#α#} + (r|σ| -s ds r {α})"
```

The next lemma establishes properties of the lexicographic maximum measure.

► **Lemma 8** ([17, Lemma 3.2]).

1.  $\gamma|\sigma| = \gamma\sigma$
2.  $\gamma|\sigma\tau| = |\sigma| + (|\tau| - s \gamma\sigma)$

**Proof.**

1. By induction on  $\sigma$ . The base case is trivial. Using Lemma 6(1) the inductive step amounts to  $\gamma\alpha \cup \gamma(|\sigma| - s \gamma\alpha) = \gamma\alpha \cup \gamma\sigma$ . The inclusion from left to right follows from the induction hypothesis. For the inclusion from right to left we proceed by case analysis. If  $x \in \gamma\alpha$  then the result immediately follows. If  $x \notin \gamma\alpha$  then clearly  $x \in \gamma\sigma$  and from the induction hypothesis  $x \in \gamma|\sigma|$ . Furthermore  $x \notin \gamma\alpha$  using Lemma 4 also yields  $x \notin \gamma(\gamma\alpha)$ . Hence  $x \in \gamma|\sigma| - s \gamma(\gamma\alpha)$  and from Lemma 6(1) we obtain  $x \in \gamma(|\sigma| - s \gamma\alpha)$ , from which the result follows.
2. By induction on  $\sigma$ , see [17]. ◀

*Decreasingness* is defined on quadruples (of labels).

► **Definition 9** ([17, Definition 3.3] for labels). The quadruple of labels  $(\tau, \sigma, \sigma', \tau')$  is *decreasing* (D) if  $|\sigma\tau'| \preceq_{\text{mul}} |\tau| + |\sigma|$  and  $|\tau\sigma'| \preceq_{\text{mul}} |\tau| + |\sigma|$ . For a visualization see Figure 1a.<sup>4</sup>

We write D into a diagram to indicate that its labels are decreasing.

This definition has a one-to-one correspondence in Isabelle:

<sup>4</sup> Although the results in Sections 3.2 and 3.3 are on labels only, for visualization we already use diagrams, although labeled rewriting will only be introduced in Section 3.4.

```

definition decreasing::"a rel  $\Rightarrow$  'a list  $\Rightarrow$  'a list  $\Rightarrow$  'a list  $\Rightarrow$  'a list  $\Rightarrow$  bool"
where "decreasing r  $\tau$   $\sigma$   $\sigma'$   $\tau'$  = ((r| $\sigma@ \tau'$ |, r| $\tau$ | + r| $\sigma$ |)  $\in$  mult_eq r
       $\wedge$  (r| $\tau@ \sigma'$ |, r| $\tau$ | + r| $\sigma$ |)  $\in$  mult_eq r)"

```

Decreasingness can also be stated differently.

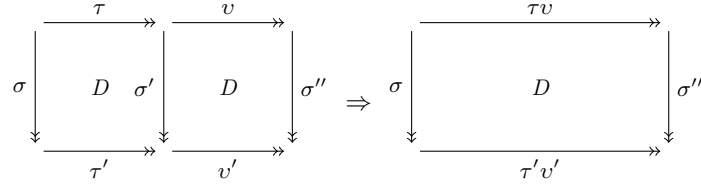
► **Lemma 10** ([17, Definition 3.3]). *The statements*

1.  $|\sigma\tau'| \preceq_{mul} |\tau| + |\sigma|$  and  $|\tau\sigma'| \preceq_{mul} |\tau| + |\sigma|$  and
  2.  $|\tau'| - s \preceq_{mul} |\tau|$  and  $|\sigma'| - s \preceq_{mul} |\tau|$
- are equivalent.

**Proof.** By Lemma 8(2) and Lemma 6(6). ◀

We have followed the (involved) proofs in [17] that pasting preserves decreasingness (Lemma 11) and that pasting is hypothesis decreasing (Lemma 12) without big changes.

► **Lemma 11** ([17, Lemma 3.5] for labels).

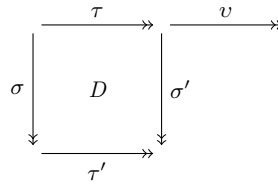


**Proof.** As in [17] except that we show  $\preceq_{mul}$  instead of  $\subseteq$  for the step

$$(|v'| - s \preceq_{mul} |\tau'|) - s \preceq_{mul} (|v'| - s \preceq_{mul} |\sigma'|) - s \preceq_{mul} |\tau|$$

where we needed Lemma 6(8) (in the last sequence in [17, Proof of Lemma 3.5]). ◀

► **Lemma 12** ([17, Lemma 3.6] for labels). *If  $\tau$  is non-empty and we have*



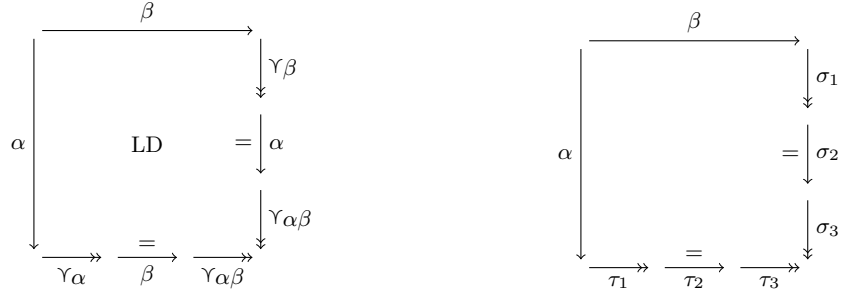
then  $|\sigma'| + |v| \prec_{mul} |\sigma| + |\tau v|$ .

**Proof.** As in [17] using Lemma 6(9) in the second step. ◀

### 3.3 Local Decreasingness

Labels in Figure 1a are *locally decreasing* (LD) if they are decreasing and both  $\sigma$  and  $\tau$  consist of exactly one label (see Figure 1b). Local decreasingness can also be formulated differently:

► **Lemma 13** ([17, Proposition 3.4]). *The form of locally decreasing labels is specified in Figure 2a.*



(a) Alternative formulation of local decreasingness. (b) Giving names to the joining sequences.

■ **Figure 2** Local diagrams.

To show the lemma we give names to the joining sequences as in Figure 2b. Then the condition of Figure 2a can be expressed as:<sup>5</sup>

$$LD' := \sigma_1 \subseteq \gamma\beta \wedge \text{length } \sigma_2 \leq 1 \wedge \sigma_2 \subseteq \{\alpha\} \wedge \sigma_3 \subseteq \gamma\alpha\beta \wedge \\ \tau_1 \subseteq \gamma\alpha \wedge \text{length } \tau_2 \leq 1 \wedge \tau_2 \subseteq \{\beta\} \wedge \tau_3 \subseteq \gamma\alpha\beta$$

Local decreasingness of the labels in the diagram of Figure 2a (using Lemma 10) amounts to the condition

$$LD := |\sigma'| - s \gamma\beta \preceq_{\text{mul}} |\alpha| \wedge |\tau'| - s \gamma\alpha \preceq_{\text{mul}} |\beta|$$

Hence Lemma 13 states that  $LD' \Leftrightarrow LD$ . This means that

- (i) if a local diagram satisfies the conditions in Figure 2a, i.e.  $LD'$ , then it is decreasing and
- (ii) local decreasingness implies that the joining sequences  $\tau'$  and  $\sigma'$  in Figure 1b can be decomposed into  $\tau_1\tau_2\tau_3$  and  $\sigma_1\sigma_2\sigma_3$  such that the properties of the local diagram in Figure 2a, i.e.  $LD'$ , are satisfied.

Lemma 15 will be the key result for (i), but first we establish a useful lemma.

► **Lemma 14.**  $|\sigma| \leq \sigma$

**Proof.** By induction on  $\sigma$ . The base case is trivial. The step case amounts to

$$|\alpha\sigma| = |\sigma| - s \gamma\alpha \leq \sigma - s \gamma\alpha \leq \alpha\sigma$$

using Definition 7 in the first step and the induction hypothesis in the second step. ◀

In the sequel we will view  $|\sigma|$  and  $\sigma$  as sets and use  $|\sigma| \subseteq \sigma$ .

Now we can prove the following key result.

► **Lemma 15.**  $\sigma_1 \subseteq \gamma\beta \wedge \text{length } \sigma_2 \leq 1 \wedge \sigma_2 \subseteq \{\alpha\} \wedge \sigma_3 \subseteq \gamma\alpha\beta \Rightarrow |\sigma_1\sigma_2\sigma_3| - s \gamma\beta \preceq_{\text{mul}} |\alpha|$

**Proof.** We show (★):

$$(|\sigma_1| - s \gamma\beta) + ((|\sigma_2| - s \gamma\sigma_1) - s \gamma\beta) + (((|\sigma_3| - s \gamma\sigma_2) - s \gamma\sigma_1) - s \gamma\beta) \preceq_{\text{mul}} \{\#\alpha\#\}$$

<sup>5</sup> Here **length** computes the length of a list.

which is equivalent to the conclusion by Lemmata 8(2), 2(1) and Definition 7. The hypothesis contains  $\sigma_1 \subseteq \gamma\beta$ , which together with Lemma 14 yields  $|\sigma_1| \subseteq \gamma\beta$  and hence

$$|\sigma_1| -s \gamma\beta = \{\#\} \quad (1)$$

Similarly from  $\sigma_3 \subseteq \gamma\alpha\beta$  we get  $|\sigma_3| -s (\gamma\alpha \cup \gamma\beta) = \{\#\}$  and hence

$$|\sigma_3| -s (\gamma\sigma_2 \cup \gamma\sigma_1 \cup \gamma\alpha \cup \gamma\beta) = \{\#\} \quad (3)$$

Using  $\text{length } \sigma_2 \leq 1 \wedge \sigma_2 \subseteq \{\alpha\}$  from the hypothesis we have two cases to consider for  $\sigma_2$ .

■ If  $\sigma_2 = []$  then

$$(|\sigma_2| -s \gamma\sigma_1) -s \gamma\beta = \{\#\} \quad (2)$$

and from (3) we have

$$((|\sigma_3| -s \gamma\sigma_2) -s \gamma\sigma_1) -s \gamma\beta \preceq_{\text{mul}} \{\#\alpha\#\} \quad (3')$$

using Lemma 2(2). Then  $(\star)$  follows immediately from (1), (2), and (3').

■ If  $\sigma_2 = [\alpha]$  then we get (2')

$$\begin{aligned} (|\sigma_2| -s \gamma\sigma_1) -s \gamma\beta &= |\sigma_2| -s (\gamma\sigma_1 \cup \gamma\beta) && \text{Lemma 2(2)} \\ &= \{\#\alpha\#\} -s (\gamma\sigma_1 \cup \gamma\beta) && \sigma_2 = [\alpha] \text{ with Definition 7} \\ &\preceq_{\text{mul}} \{\#\alpha\#\} && \text{Lemma 6(8)} \end{aligned}$$

and (because  $\gamma\sigma_2 = \gamma\alpha$ ), similar as in the other case from (3) we get

$$((|\sigma_3| -s \gamma\sigma_2) -s \gamma\sigma_1) -s \gamma\beta = \{\#\} \quad (3'')$$

From (1), (2'), and (3'') we conclude  $(\star)$ .  $\blacktriangleleft$

Next we prepare for the key lemma to establish (ii), i.e., Lemma 17, after establishing useful intermediate results. Note that Lemma 16(2) can be seen as an inverse of Lemma 14.

► **Lemma 16.**

1.  $\alpha \in \#|\sigma| \Rightarrow \exists \sigma_1 \sigma_3. \sigma = \sigma_1 \alpha \sigma_3 \wedge \alpha \notin \# \gamma\sigma_1$
2.  $|\sigma| \subseteq \gamma S \Rightarrow \sigma \subseteq \gamma S$
3.  $S \subseteq \gamma T \Rightarrow \gamma S \subseteq \gamma T$

**Proof.**

1. By induction on  $\sigma$ . The base case is trivial. In the step case we can assume that  $\alpha \in \#|\beta\sigma|$ . We proceed by case analysis.
  - If  $\alpha = \beta$  then we are done with  $\sigma_1 = []$  and  $\sigma_3 = \sigma$ .
  - In the other case we have  $\alpha \in \#|\sigma|$  and  $\alpha \notin \# \gamma\beta$  from Definition 7. The induction hypothesis yields  $\sigma'_1$  and  $\sigma'_3$  with  $\sigma = \sigma'_1 \alpha \sigma'_3$  such that  $\alpha \notin \gamma\sigma'_1$ . Because  $\alpha \notin \# \gamma\beta$  we can conclude with  $\sigma_1 = \beta\sigma'_1$  and  $\sigma_3 = \sigma'_3$  using Lemma 6(1).
2. Assume  $\alpha \in \sigma$ . If  $\alpha \in \#|\sigma|$  then we are done by the hypothesis. In the other case there must be a  $\beta \in |\sigma|$  (easy induction on  $\sigma$ ) with  $\alpha \prec \beta$ . From the hypothesis we get that  $\beta \in \gamma S$  and by transitivity also  $\alpha \in \gamma S$ , which finishes the proof.
3. We assume  $s \in \gamma S$ . If  $s \in S$  then the hypothesis finishes the proof. In the other case there is a  $y \in S$  with  $x \prec y$ . The hypothesis yields  $y \in \gamma T$ . From this we obtain a  $z \in T$  with  $y \prec z$ . By transitivity of  $\prec$  we get  $x \prec z$ , which shows the result.  $\blacktriangleleft$



With these additional lemmata we can now prove the following key result.

► **Lemma 17.**  $|\sigma'| -s \gamma\beta \preccurlyeq_{mul} \{\#\alpha\#\} \Rightarrow \exists \sigma_1 \sigma_2 \sigma_3. \sigma' = \sigma_1 \sigma_2 \sigma_3 \wedge \sigma_1 \subseteq \gamma\beta \wedge \text{length } \sigma_2 \leq 1 \wedge \sigma_2 \subseteq \{\alpha\} \wedge \sigma_3 \subseteq \gamma\alpha\beta$

**Proof.** To show the result we perform a case analysis.

- If  $\alpha \in \#|\sigma'| -s \gamma\beta$  then Lemma 16(1) yields  $\sigma_1$  and  $\sigma_3$  with  $\sigma' = \sigma_1 \alpha \sigma_3$  and  $\alpha \notin \gamma\sigma_1$ . Hence from the hypothesis and Lemma 8(2) we get

$$(|\sigma_1| -s \gamma\beta) + \{\#\alpha\#\} + (((|\sigma_3| -s \gamma\alpha) -s \gamma\sigma_1) -s \gamma\beta) \preccurlyeq_{mul} \{\#\alpha\#\}$$

and since  $\alpha \notin \gamma\sigma_1$  and  $\alpha \notin \gamma\beta$  it follows that

$$|\sigma_1| -s \gamma\beta = \{\#\} \text{ and } ((|\sigma_3| -s \gamma\alpha) -s \gamma\sigma_1) -s \gamma\beta = \{\#\}$$

Now, Lemma 2(2) yields

$$|\sigma_1| \subseteq \gamma\beta \text{ and } |\sigma_3| \subseteq \gamma\alpha \cup \gamma\sigma_1 \cup \gamma\beta$$

and from Lemma 16(2) we get

$$\sigma_1 \subseteq \gamma\beta \text{ and } \sigma_3 \subseteq \gamma\alpha \cup \gamma\sigma_1 \cup \gamma\beta$$

The latter simplifies to  $\sigma_3 \subseteq \gamma\alpha\beta$  using  $\gamma\sigma_1 \subseteq \gamma\beta$  (from Lemma 16(3)) and Lemma 6(1). Hence in this case the result follows with  $\sigma_2 = [\alpha]$ .

- If  $\alpha \notin \#|\sigma'| -s \gamma\beta$

$$\begin{aligned} \Rightarrow |\sigma'| -s \gamma\beta &\subseteq \gamma\alpha && \text{hypothesis} \\ \Rightarrow |\sigma'| &\subseteq \gamma\alpha\beta && \text{Lemma 6(1)} \\ \Rightarrow \sigma' &\subseteq \gamma\alpha\beta && \text{Lemma 16(2)} \end{aligned}$$

In the second case the result follows with empty  $\sigma_1$  and  $\sigma_2$  and  $\sigma' = \sigma_3$ . ◀

Now Lemma 13 follows from Lemma 15 ( $LD' \Rightarrow LD$ ) and Lemma 17 ( $LD \Rightarrow LD'$ ).

### 3.4 Labeled Rewriting

So far all proofs have been on sequences of labels. However for the main result (Section 3.6) we need labeled rewriting. Hence this section sketches how we formalized *labeled* (abstract) rewriting<sup>6</sup> before lifting the results from Section 3.2 from labels to labeled rewriting.

In the sequel objects will have type 'a and labels will have type 'b. Recall that a labeled rewrite step carries the label between its two objects and is hence of type 'a × 'b × 'a. A labeled ARS is a set of labeled rewrite steps.

```
type_synonym ('a,'b) lars = "('a × 'b × 'a) set"
```

Next we define (labeled rewrite) sequences, i.e., for each object  $a$  there is the empty sequence  $a \xrightarrow{[]}$  and if  $a \xrightarrow{\alpha} b$  is a labeled rewrite step and  $b \xrightarrow{\sigma} c$  is a sequence then  $a \xrightarrow{\alpha\sigma} c$  is a sequence.

<sup>6</sup> Note that `Abstract_Rewriting.thy` does not contain any support for labeled abstract rewrite systems.

```

type_synonym ('a,'b) seq = "('a × ('b × 'a) list)"

inductive_set seq :: "('a,'b) lars ⇒ ('a,'b) seq set" for B where
  "(a, []) ∈ seq B"
  | "(a, α, b) ∈ B ⇒ (b, ss) ∈ seq B ⇒ (a, (α, b) # ss) ∈ seq B"

```

► **Example 18.** Let  $\mathcal{B}$  be the labeled ARS with the labeled relation  $\{(a, \alpha, b), (b, \beta, c)\}$ . Then  $a \xrightarrow{\alpha} b \xrightarrow{\beta} c$  (or  $a \xrightarrow{\alpha\beta} c$ ) is a sequence in  $\mathcal{B}$ , represented as  $(a, [(\alpha, b), (\beta, c)])$  in Isabelle. Empty sequences consist of at least an object, i.e., the empty sequence starting from  $a$  is  $(a, [])$ .

We introduce a function `lst`, which returns the *last* element of a rewrite sequence.

```

definition lst :: "('a,'b) seq ⇒ 'a"
where "lst ss = (if snd ss = [] then fst ss else snd (last (snd ss)))"

```

We prove useful properties for rewrite sequences, i.e., that chopping off a segment of a sequence again yields a sequence and that two sequences can be concatenated (provided the last element of the first sequence coincides with the first element of the second sequence).

- **Lemma 19.** Let  $a_1 \xrightarrow{\alpha_1} \dots \xrightarrow{\alpha_{n-1}} a_n$  and  $b_1 \xrightarrow{\beta_1} \dots \xrightarrow{\beta_{m-1}} b_m$  be sequences.
1. Then  $a_1 \xrightarrow{\alpha_1} \dots \xrightarrow{\alpha_{i-1}} a_i$  and  $a_i \xrightarrow{\alpha_i} \dots \xrightarrow{\alpha_{n-1}} a_n$  are sequences for any  $1 \leq i \leq n$ .
  2. If  $a_n = b_1$  then  $a_1 \xrightarrow{\alpha_1} \dots \xrightarrow{\alpha_{n-1}} a_n = b_1 \xrightarrow{\beta_1} \dots \xrightarrow{\beta_{m-1}} b_m$  is a sequence.

**Proof.** By induction on  $a_1 \xrightarrow{\alpha_1} \dots \xrightarrow{\alpha_{n-1}} a_n$ . ◀

As a next step we introduce diagrams.

► **Definition 20.** A *diagram* is a quadruple of sequences  $(\xrightarrow{\tau}, \xrightarrow{\sigma}, \xrightarrow{\sigma'}, \xrightarrow{\tau'})$  such that the start and endpoints of the sequences satisfy the picture in Figure 1a. A diagram is called *decreasing* if its labels are.

From now on we use  $\tau, \sigma$ , etc. also to denote (labeled rewrite) sequences in Isabelle. The type information clarifies if labels or rewrite sequences are meant.

```

definition diagram ::
  "('a,'b) lars ⇒ ('a,'b) seq × ('a,'b) seq × ('a,'b) seq × ('a,'b) seq ⇒ bool"
where "diagram B d = (let (τ, σ, σ', τ') = d in {σ, τ, σ', τ'} ⊆ seq B ∧
  fst σ = fst τ ∧ lst σ = fst τ' ∧ lst τ = fst σ' ∧ lst σ' = lst τ')"

```

Next we introduce a function `labels`, which extracts the labels of a sequence, e.g.,  $\text{labels}(a \xrightarrow{\alpha} b \xrightarrow{\beta} c) = [\alpha, \beta]$ . With the help of this function we can define a predicate `DD`, which holds if a quadruple of sequences forms a decreasing diagram.

```

definition labels ::
  "('a,'b) seq ⇒ ('a,'b) seq × ('a,'b) seq × ('a,'b) seq × ('a,'b) seq ⇒ list"
where "labels ss = map fst (snd ss)"

definition DD :: "('a,'b) lars ⇒ 'b rel ⇒ bool"
where "DD B r d = (let (τ, σ, σ', τ') = d in
  diagram B d ∧ decreasing r (labels τ) (labels σ) (labels σ') (labels τ'))"

```

We lift Lemma 11 from labels to diagrams.

► **Lemma 21** ([17, Lemma 3.5] for decreasing diagrams). *Pasting two decreasing diagrams yields a decreasing diagram. For a picture see Lemma 11.*

**Proof.** With the help of Lemma 19(2) we show that pasting two diagrams again yields a diagram. That pasting preserves decreasingness follows from Lemma 11. ◀

### 3.5 Well-Foundedness

To prove the main result we introduce a measure on *peaks* (more precisely the measure is on pairs of sequences).

► **Definition 22.** Let  $|(\xrightarrow{\tau}, \xrightarrow{\sigma})| := |\tau| + |\sigma|$ . Then we can lift  $\prec$  as a relation on labels to a relation on pairs of sequences, i.e.,  $p_1 \prec_{\text{peak}} p_2$  if  $|p_1| \prec_{\text{mul}} |p_2|$ .

```
definition measure :: "'b rel  $\Rightarrow$  ('a,'b) seq  $\times$  ('a,'b) seq  $\Rightarrow$  'b multiset"
  where "measure r p = r|labels (fst p)| + r|labels (snd p)|"

definition pex :: "'b rel  $\Rightarrow$  ('a,'b) seq  $\times$  ('a,'b) seq"
  where "pex r = {(p1,p2). (measure r p1, measure r p2)  $\in$  mul r}"
```

For proofs of induction we establish that  $\prec_{\text{peak}}$  is well-founded.

► **Lemma 23.** *Let  $\prec$  be well-founded. Then  $\prec_{\text{peak}}$  is well-founded.*

**Proof.** From [4] we get that  $\prec_{\text{mul}}$  is well-founded (this proof is contained in `Multiset.thy`). We proceed by contraposition. Assume the measure on peaks is not well-founded. Then we obtain an infinite sequence

$$\cdots \prec_{\text{peak}} (\tau_2, \sigma_2) \prec_{\text{peak}} (\tau_1, \sigma_1)$$

which entails an infinite sequence on multisets

$$\cdots \prec_{\text{mul}} |\tau_2| + |\sigma_2| \prec_{\text{mul}} |\tau_1| + |\sigma_1|$$

showing the result. ◀

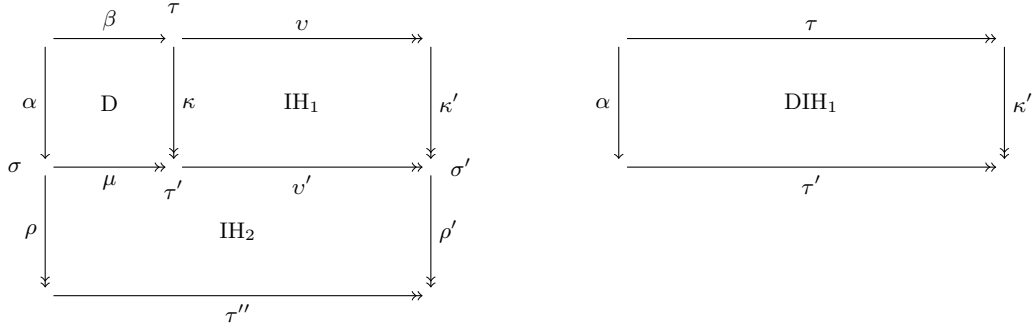
### 3.6 Main Result

► **Definition 24.** A *peak* is a pair of labeled rewrite sequences which originate from the same object. A *local peak* is a peak where the labeled rewrite sequences consist of a single step.

```
definition peak :: "('a,'b) lars  $\Rightarrow$  ('a,'b) seq  $\times$  ('a,'b) seq  $\Rightarrow$  bool"
  where "peak lars p = (let ( $\tau, \sigma$ ) = p in  $\{\tau, \sigma\} \subseteq$  seq lars  $\wedge$  fst  $\tau$  = fst  $\sigma$ )"

definition local_peak :: "('a,'b) lars  $\Rightarrow$  ('a,'b) seq  $\times$  ('a,'b) seq  $\Rightarrow$  bool"
  where "local_peak lars p = (let ( $\tau, \sigma$ ) = p in
    peak lars p  $\wedge$  length (snd  $\tau$ ) = 1  $\wedge$  length (snd  $\sigma$ ) = 1)"
```

► **Definition 25.** A peak  $(\xrightarrow{\tau}, \xrightarrow{\sigma})$  in a labeled ARS  $\mathcal{B}$  is *decreasing* if it can be completed into a decreasing diagram, i.e., there are  $\xrightarrow{\sigma'}$  and  $\xrightarrow{\tau'}$  such that the conditions of Figure 1a are satisfied. A peak is *locally decreasing*, if it is decreasing and a local peak.



(a) Local decreasingness implies decreasingness.

(b) Pasting  $D$  and  $IH_1$  into  $DIH_1$ .■ **Figure 3** Lemma 26

We establish that if all local peaks of a labeled ARS  $\mathcal{B}$  are decreasing then all peaks of  $\mathcal{B}$  are decreasing, following the structure of the proof of [17, Theorem 3.7]. (Changes are discussed in Section 4). Note that only here we need that  $\prec$  is well-founded, from which irreflexivity immediately follows (to satisfy our global assumption from Section 2).

► **Lemma 26** (similar to [17, Theorem 3.7]). *Let  $\mathcal{B}$  be a labeled ARS and  $\prec$  be a transitive and well-founded order on the labels. If all local peaks of  $\mathcal{B}$  are decreasing, then all peaks of  $\mathcal{B}$  are decreasing.*

**Proof.** To show that all peaks are decreasing we fix a peak  $(\xrightarrow{\tau}, \xrightarrow{\sigma})$  and show that this peak can be completed into a decreasing diagram. The proof is by well-founded induction on  $\prec_{\text{peak}}$  and there only is the step case. The only interesting situation is when neither  $\tau$  nor  $\sigma$  are empty, i.e., (using Lemma 19(1) we obtain)  $\xrightarrow{\tau} = \xrightarrow{\beta} \cdot \xrightarrow{v}$  and  $\xrightarrow{\sigma} = \xrightarrow{\alpha} \cdot \xrightarrow{\rho}$  (see Figure 3a). Hence  $(\xrightarrow{\beta}, \xrightarrow{\alpha})$  is a local peak and from the assumption we obtain a decreasing diagram with joining sequences  $\xrightarrow{\kappa}$  and  $\xrightarrow{\mu}$ . We obtain that  $(\xrightarrow{v}, \xrightarrow{\kappa})$  is a peak and want to show that the measure of this peak is smaller than that of  $(\xrightarrow{\tau}, \xrightarrow{\sigma})$  (to apply the induction hypothesis). Since  $\beta$  is not empty with Lemma 12 we establish that  $|(\xrightarrow{v}, \xrightarrow{\kappa})|$  is smaller than  $|(\xrightarrow{\tau}, \xrightarrow{\sigma})|$  and from  $|\alpha| \prec_{\text{mul}} |\sigma|$ <sup>7</sup> we obtain the desired result. Now, the induction hypothesis yields that  $IH_1$  is a decreasing diagram. Concatenating (using Lemma 19(2))  $\xrightarrow{\mu}$  and  $\xrightarrow{v'}$  into a sequence  $\xrightarrow{\tau'}$ , using Lemma 21 we can paste the diagrams  $D$  and  $IH_1$  into a decreasing diagram ( $DIH_1$ , see Figure 3b).

The peak  $(\xrightarrow{\tau'}, \xrightarrow{\rho})$  is smaller than the peak  $(\xrightarrow{\tau}, \xrightarrow{\sigma})$  by a mirrored version of Lemma 12 and hence the induction hypothesis yields the decreasing diagram  $IH_2$ . Finally, a mirrored version of Lemma 21 pastes  $DIH_1$  and  $IH_2$  into a decreasing diagram, concluding the proof. ◀

We define local decreasingness for ARSs.

► **Definition 27** ([17, Definition 3.8]). An ARS  $\mathcal{A}$  is *locally decreasing* if there exists a transitive and well-founded relation  $\prec$  on the labels such that all local peaks are decreasing for (a labeled version of)  $\mathcal{A}$ .

<sup>7</sup> This step is missing in [17].

The corresponding definition in Isabelle shows that the labeled version of  $\mathcal{A}$  can be chosen freely since we only demand the existence of a labeled version of  $\mathcal{A}$  satisfying decreasingness of all local peaks.

```

definition unlabeled :: "('a,'b) lars  $\Rightarrow$  'a rel"
where "unlabeled  $\mathcal{B}$  = {(a,c).  $\exists b. (a,b,c) \in \mathcal{B}$ }"

definition LD :: "'b  $\Rightarrow$  'a rel  $\Rightarrow$  bool"
where "LD L  $\mathcal{A}$  = ( $\exists r \mathcal{B}. (\mathcal{A} = \text{unlabeled } \mathcal{B}) \wedge \text{trans } r \wedge \text{wf } r \wedge$ 
 $(\forall p. (\text{local\_peak } \mathcal{B} p \longrightarrow (\exists \sigma' \tau'. (\text{DD } \mathcal{B} r (\text{fst } p, \text{snd } p, \sigma', \tau'))))))$ )"

```

Finally we arrive at the main result for soundness:

► **Corollary 28** ([17, Corollary 3.9]). *A locally decreasing ARS is confluent.*

**Proof.** From local decreasingness we get a transitive and well-founded relation  $\prec$  such that all local peaks are decreasing in a labeled version of the ARS. Lemma 26 yields that all peaks are decreasing. The result follows by dropping labels from the labeled rewrite sequences. ◀

### 3.7 Applications

To show the applicability of our formalization we have formally proven Newman’s Lemma:

► **Lemma 29.** *A locally confluent and terminating ARS is confluent.*

**Proof.** We follow the proof in [17]. As labeled ARS we take  $\mathcal{A}' = \{(a, a, b) \mid (a, b) \in \mathcal{A}\}$  and as relation on the labels we use  $\prec = \leftarrow^+$ . From termination of  $\rightarrow$  we get well-foundedness and transitivity of  $\prec$ .

Next we establish that  $a \rightarrow a_1 \rightarrow a_2 \rightarrow \dots$  implies  $a_i \prec a$  for any  $i \geq 1$  by induction on the labeled rewrite sequence (using transitivity of  $\prec$ ).

Hence from Lemma 13 and the local confluence assumption we get decreasingness of all local peaks. The result follows from Lemma 26 and Corollary 28. ◀

## 4 Meanderings

In this section we discuss differences between our formalization and (proofs from) [17].

Within Isabelle an ARS is just a binary relation while in [17] the ARS also contains the domain of the relation. A similar statement holds for labeled ARSs.

*General multisets* are used in [17], which can represent sets and finite multisets in one go whereas our formalization clearly separates the two concepts. This allows to reuse existing machinery from the Isabelle theories `Set.thy` and `Multiset.thy`. The separation of both concepts did not blow up our formalization, only for the definition of the down-set and for Lemma 6(1) we needed such duplicates.

However, [17] uses a different definition of the multiset extension than `Multiset.thy` where the multiset extension is defined as the transitive closure of the “one-step” multiset extension.

► **Definition 30** (`Multiset.thy`). The *one-step multiset extension* (denoted by  $\prec_{\text{mult1}}$ ) of  $\prec$  is defined by

$$M \prec_{\text{mult1}} N \text{ if } \exists a \ I \ K. M = I + K, N = I + \{\#a\#\}, \forall b \in K. b \prec a$$

and the *multiset extension* of  $\prec$  (denoted by  $\prec_{\text{mult}}$ ) is the transitive closure of  $\prec_{\text{mult1}}$ .

Based on the results in `Multiset.thy` and Definition 3(1) we have proven these two definitions equivalent for any transitive base relation.

► **Lemma 31.** *If  $\prec$  is transitive then  $\prec_{mult}$  and  $\prec_{mul}$  coincide.* ◀

Moreover we proved the claim in Definition 3.

► **Lemma 32.** *We have that  $\preceq_{mul}$  is the reflexive closure of  $\prec_{mul}$ .* ◀

**Proof.** First we show the inclusion from left to right. Let  $(M, N) \in \preceq_{mul}$ . If  $J = \{\#\}$  then  $M = N$  and the result follows. In the other case  $(M, N) \in \prec_{mul}$  and we are done.

For the reverse inclusion let  $(M, N)$  be in the reflexive closure of  $\prec_{mul}$ . If  $M = N$  then we finish with  $I = M$ ,  $K = J = \{\#\}$ . In the other case we get suitable  $I$ ,  $J$ , and  $K$  from the definition of  $\prec_{mul}$ . ◀

Our formalization is first performed for sequences (of labels) and then lifted to labeled rewrite sequences, a step which is left implicit in [17].

Next we want to stress that our proofs of Lemmata 6(3) and Lemma 8(1) differ from the informal ones in [17]. Since Lemma 13 is stated as a proposition in [18], the informal argument given there could not be replayed directly in Isabelle. Hence we also contributed a formal proof of this result, requiring auxiliary results (Lemmata 14 and 16).

Concerning missing proofs (or proof steps), we mention Lemma 6(8,9), which we needed to replay the proofs of Lemmata 11 and 12.

There are some (tiny) differences between [17, Main Theorem 3.7] and Lemma 26. [17] claims to use a measure on diagrams. However, since the closing/joining steps of the diagram are just obtained by the induction hypothesis a measure on peaks seems more suitable. Moreover, since in either case the measure is a multiset it is hard to relate arbitrary multisets to a peak. Hence we lifted the order on labels  $\prec$  to peaks  $\prec_{peak}$  (Section 3.5) and used well-founded induction on this order. In the formalization of Lemma 26 (Footnote 7) we located a missing step, which is essential to apply the induction hypothesis. Another aspect where our formalization deviates from [17] is that the original work uses families of labeled ARSs whereas our formalization considers a single labeled ARS only. Hence [17, Theorem 3.7] states the main result on families of ARSs whereas our Lemma 26 makes a statement about a single ARS.

All in all we regard the *gaps* that we spotted to mainly be gaps for a theorem prover, while a human would easily swallow them. Furthermore we want to stress that the precision (while compactness) of the proofs given in [17] clearly helped us in the task of formalizing its main theorem.

## 5 Conclusion

In this paper we have described a formalization of decreasing diagrams in the theorem prover Isabelle following the original proof from [17]. Our contribution is more than just replaying the proofs in Isabelle, e.g., the results of Sections 3.3, 3.4 and 3.5 are either informal or implicit in [17]. Note that some of our achievements on multisets (especially Lemma 6(3)) are of interest for a larger community.

In [2] a “point version” of decreasing diagrams is introduced, where objects are labeled instead of steps. It is unknown if the point version is equivalent to the standard one. Parts of [2] have been formalized in Coq but 29 axioms are assumed, i.e., not proven in the theorem prover. Furthermore the more useful alternative representation of local decreasingness

(Lemma 13) is not considered in [2]. Hence for these reasons we do not regard [2] as a (complete) formalization of decreasing diagrams.

We anticipate that our contribution paves the way for future work in several directions. One possibility is the formalization of confluence results that can be proven with decreasing diagrams (e.g. Toyama’s theorem [20]). Another idea would be the certification of confluence proofs (based on decreasing diagrams) given by automated confluence provers. Both aims will require to lift our formalization of decreasing diagrams from abstract rewriting to term rewriting. We stress that the *Isabelle Formalization of Rewriting* (IsaFoR [30]) already contains notions such as critical pairs, which will ease this job. IsaFoR has been developed to formalize termination criteria for rewriting and also offers the opportunity to check concrete termination proofs given by automated termination tools. A dedicated category is present in the international competition of termination tools<sup>8</sup> since 2007. Concerning the confluence competition,<sup>9</sup> already in its first edition confluence proofs due to Knuth and Bendix’ criterion [12] and for orthogonal systems [22] could be certified with the help of IsaFoR. These two criteria applied to 27 out of 113 confluence proofs and hence our contribution can be seen as a first step to drastically increase the number of certified confluence proofs.

Finally we remark that we will formalize alternative proofs of decreasing diagrams. While the conversion version of decreasing diagrams [19] in theory is equally powerful as the one from [17], practice has shown a slightly different picture [8]. Since the proof of the conversion version of decreasing diagrams follows the structure of Lemma 26, we anticipate that our formalization forms a good basis for this challenge.

## Acknowledgments

We thank Bertram Felgenhauer for contributing an initial proof of a part of Lemma 6(3) and for locating the formalization of [2]. He, Nao Hirokawa, and Aart Middeldorp also commented on earlier versions of this paper.

---

## References

- 1 Bezem, M., Klop, J., V. van Oostrom: Diagram techniques for confluence. I&C 141(2), 172–204 (1998)
- 2 Bognar, M.: A point version of decreasing diagrams. In: Engelfriet, J., Spaan, T. (eds.) Proc. Accolade ’96, Dutch Graduate School in Logic. pp. 1–14 (1997). Available from <http://web.archive.org/web/20051226052550/http://www.cs.vu.nl/~mirna/>
- 3 Contejean, E., Courtieu, P., Forest, J., Pons, O., Urbain, X.: Automated certified proofs with CiME3. In: Proc. 22nd RTA. LIPIcs, vol. 10, pp. 21–30 (2011)
- 4 Dershowitz, N., Manna, Z.: Proving termination with multiset orderings. Commun. ACM 22(8), 465–476 (1979)
- 5 Felgenhauer, B.: A proof order for decreasing diagrams. In: Proc. 1st IWC. pp. 7–13 (2012)
- 6 Galdino, A., Ayala-Rincón, M.: A formalization of Newman’s and Yokouchi’s lemmas in a higher-order language. JFR 1(1), 39–50 (2008)
- 7 Galdino, A.L., Ayala-Rincón, M.: A formalization of the knuth-bendix(-huet) critical pair theorem. J. Autom. Reasoning 45(3), 301–325 (2010)

---

<sup>8</sup> <http://termcomp.uibk.ac.at>

<sup>9</sup> <http://coco.nue.riec.tohoku.ac.jp/>

- 8 Hirokawa, N., Middeldorp, A.: Decreasing diagrams and relative termination. *JAR* 47(4), 481–501 (2011)
- 9 Huet, G.: Residual theory in lambda-calculus: A formal development. *JFP* 4(3), 371–394 (1994)
- 10 Jouannaud, J.P., van Oostrom, V.: Diagrammatic confluence and completion. In: *Proc. 36th ICALP. LNCS*, vol. 5556, pp. 212–222 (2009)
- 11 Klop, J., van Oostrom, V., de Vrijer, R.: A geometric proof of confluence by decreasing diagrams. *JLP* 10(3), 437–460 (2000)
- 12 Knuth, D., Bendix, P.: Simple word problems in universal algebras. In: Leech, J. (ed.) *Computational Problems in Abstract Algebra*, 263–297. Pergamon Press (1970)
- 13 Newman, M.: On theories with a combinatorial definition of equivalence. *Annals of Mathematics* 43(2), 223–243 (1942)
- 14 Nipkow, T.: More Church-Rosser proofs. *JAR* 26(1), 51–66 (2001)
- 15 Nipkow, T., Paulson, L., Wenzel, M.: Isabelle/HOL – A Proof Assistant for Higher-Order Logic. vol. 2283 of *LNCS*. Springer (2002)
- 16 van Oostrom, V.: (Decreasing proof orders – interpreting conversions in involutive monoids)
- 17 van Oostrom, V.: Confluence by decreasing diagrams. *TCS* 126(2), 259–280 (1994)
- 18 van Oostrom, V.: Developing developments. *TCS* 175(1), 159–181 (1997)
- 19 van Oostrom, V.: Confluence by decreasing diagrams – converted. In: *Proc. 19th RTA. LNCS*, vol. 5117, pp. 306–320 (2008)
- 20 van Oostrom, V.: Modularity of confluence constructed. In: *Proc. 4th IJCAR. LNCS*, vol. 5195, pp. 348–363 (2008)
- 21 Pol, J.: Modularity in many-sorted term rewriting systems. Master’s thesis, report INF/SCR-92-37, Utrecht University (1992)
- 22 Rosen, B.: Tree-manipulating systems and Church-Rosser theorems. *JACM* 20(1), 160–187 (1973)
- 23 Ruiz-Reina, J.L., Alonso, J.A., Hidalgo, M.J., Martín-Mateos, F.J.: Formal proofs about rewriting using ACL2. *AMAI* 36(3), 239–262 (2002)
- 24 Shankar, N.: A mechanical proof of the Church-Rosser theorem. *JACM* 35(3), 475–522 (1988)
- 25 Sternagel, C., Thiemann, R.: Abstract rewriting. *Archive of Formal Proofs* 2010 (2010)
- 26 Støvring, K.: Extending the extensional lambda calculus with surjective pairing is conservative. *Logical Methods in Computer Science* 2(2), 14 pages (2006)
- 27 Takahashi, M.: Parallel reductions in  $\lambda$ -calculus. *I&C* 118(1), 120–127 (1995)
- 28 Terese: *Term Rewriting Systems*. vol. 55 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press (2003)
- 29 Thiemann, R.: Certification of confluence proofs using CeTA. In: *Proc. 1st IWC*. pp. 45–45 (2012)
- 30 Thiemann, R., Sternagel, C.: Certification of termination proofs using CeTA. In: *Proc. 22nd TPHOLs. LNCS*, vol. 5674, pp. 452–468 (2009)